UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/612,198	07/01/2003	Carey Nachenberg	20423-07775	4107

34415 7590 08/25/2008

SYMANTEC/ FENWICK
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	PAPER NUMBER
2137	

NOTIFICATION DATE	DELIVERY MODE
08/25/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptoc@fenwick.com
bhoffman@fenwick.com
aprice@fenwick.com

Office Action Summary	Application No.	Applicant(s)	
	10/612,198	NACHENBERG ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 May 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3,4,6-11,13-16 and 18-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3,4,6-11,13-16 and 18-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *20080226*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A response was received on 08 May 2008. By this response, Claims 1, 3, 4, 6, 7, 10, 11, 13, 14, 16, and 18-20 have been amended. Claims 5, 12, and 17 have been canceled. New Claims 22-24 have been added. Claims 1, 3, 4, 6-11, 13-16, and 18-24 are currently pending in the present application.

Response to Arguments

2. Applicant's arguments with respect to claims 20 and 22 have been considered but are moot in view of the new ground(s) of rejection.

3. Applicant's arguments filed 08 May 2008 have been fully considered but they are not persuasive.

Regarding the rejection of Claims 1 and 3-21 under 35 U.S.C. 103(a) as unpatentable over Applicant admitted prior art in view of Ramarao et al, US Patent Application Publication 2004/0199647, and Gruper et al, US Patent 7047369, in response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Specifically, regarding independent Claims 1 and 16 as amended, Applicant separately argues that neither Gruper nor Ramarao discloses performing a statistical

analysis of categories and ending a training phase responsive to the statistical analysis (pages 10-11 and 12 of the present response). The Examiner respectfully disagrees, noting that at least Gruper explicitly discloses several statistical methods by which the duration of the training phase may be determined (see Gruper, column 2, lines 50-63, where the length of the learning phase may be based on a measure of time or a predetermined number or operations or a predetermined number of new operations is learned) and also suggests that any alternatives to determining limitations on the training phase may be used (Gruper, column 2, lines 59-62).

Further regarding independent Claims 1 and 16, Applicant separately argues that neither Gruper nor Ramarao discloses the limitation of "grouping the commands into categories", and also regarding independent Claim 21, Applicant separately argues that neither Gruper nor Ramarao discloses the limitation of "grouping the commands responsive to the commands' canonical forms". In particular, Applicant argues that a cited portion of Gruper does not disclose the above noted "grouping" limitation (page 11 of the present response). However, the Examiner notes that Gruper was not explicitly relied upon for a teaching of such a limitation with respect to Claim 21, and the other independent Claims did not previously recite such a grouping limitation; instead, Ramarao was relied upon for disclosure of grouping commands according to their canonical forms (see page 9 of the previous Office action, citing paragraph 0032 of Ramarao). Applicant further separately alleges that Ramarao does not disclose the claimed "grouping" but points to no evidence in support of this allegation; this argument fails to comply with 37 CFR 1.111(b) because it amounts to a general allegation that the

claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

Therefore, for the reasons detailed above, the Examiner maintains the rejection as set forth below.

Specification

4. The objection to the disclosure for informalities is NOT withdrawn. With respect to the statement in the previous Office action that on page 7, line 26, or the specification, it appears that "commend" is intended to read "command", although Applicant alleges that "this portion of the specification does not contain the typographical error suggested by the Examiner" (page 8 of the present response), the Examiner notes that the sentence at lines 25-26 of page 7 of the specification clearly reads "In other words, set 6 is updated **commend**-by-command" (emphasis added). Therefore the error is, in fact, present, and must be corrected.

5. The disclosure is objected to because of the following informalities:

The specification appears to contain minor typographical and other errors. For example, on page 7, line 26, it appears that "commend" is intended to read "command".

Appropriate correction is required. Applicant's cooperation is requested in correcting any other errors of which applicant may become aware in the specification.

Claim Objections

6. The objection to Claim 10 for informalities is withdrawn in light of the amendments to the Claims.

Claim Rejections - 35 USC § 101

7. The rejection of Claim 20 under 35 U.S.C. 101 as directed to non-statutory subject matter is withdrawn in light of the amendments to the claims.

Claim Rejections - 35 USC § 112

8. The rejection of Claims 3, 4, 6, and 11 under 35 U.S.C. 112, second paragraph, as indefinite is withdrawn in light of the amendments to the claims.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 1, 3, 4, 6-11, 13-16, 18, 19, 21, 23, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Applicant admitted prior art, in view of Ramaro et al, US Patent Application Publication 2004/0199647, Gruper et al, US Patent 7047369.

In reference to Claim 1, Applicant admits as prior art the general use of database intrusion detection systems (see page 1, lines 4-17 of the present specification). However, Applicant does not admit the use of real time training of such a database intrusion detection system.

Ramarao discloses a method in which an intrusion detection system has derived a set of acceptable commands (see paragraphs 0056-0057, where there is a list of allowed actions; see also paragraph 0066, where the access control software can be implemented as part of an intrusion detection system) and groups commands into categories (paragraph 0032, where commands are generalized using variables and grouped accordingly). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the access control portion of the intrusion detection system (IDS) of Ramarao into the admitted prior art database intrusion detection system, because the application of the general IDS principles disclosed by Ramarao to the admitted prior art database IDS would yield the predictable result of increasing the security of the admitted prior art database IDS by preventing unauthorized actions (see Ramarao, paragraph 0027). However, Ramarao does not explicitly disclose that commands are observed in real time before deriving the set of acceptable commands.

Gruper discloses a method in which a security system includes a learning mode in which commands are observed in order to compile an enforcement file of acceptable actions and commands are grouped into categories (column 5, lines 32-61, where commands and access rights are grouped into enforcement files by program), and in which a statistical analysis is performed of the categories and the training phase is ended responsive to that statistical analysis (column 2, lines 50-63, where a time period or number of operations learned is analyzed and used to determine the length of the learning mode). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the real-time learning mode of Gruper into the admitted prior art database IDS as modified by Ramarao, in order to allow a system to gradually build up knowledge of what actions are and are not to be allowed (see Gruper, column 5, lines 32-47).

In reference to Claim 3, Official notice is taken that it is well-known in the art to use SQL commands when accessing a database. Therefore, it would have been obvious to one of ordinary skill in the art to apply the method of Claim 1 when SQL commands are being used to provide the security to the database that uses SQL.

In reference to Claim 4, the cited art further discloses at least one command is a query, an add, a delete, or a modify (see Gruper, column 4, lines 49-64, Table 1; see also Ramarao, paragraphs 0004-0005).

In reference to Claims 6 and 7, the cited art further discloses that at least one category includes canonicalized commands having commands stripped of literal field data (see Ramarao, paragraph 0032, where parameters can be configured as variable).

In reference to Claims 8-10, the cited art further discloses auditing and extracting commands by at least one of an API, code injection, patching, or direct integration (Gruper, column 5, lines 7-61) and in-line interception using at least a proxy, firewall, or sniffer (Ramarao, paragraph 0037).

In reference to Claim 11, the cited art further discloses tracking and reporting suspicious activity (Ramarao, paragraph 0066; Gruper, column 4, line 65-column 5, line 6).

In reference to Claim 13-15, the cited art further discloses an operational phase in which commands that access the database are compared to the set of acceptable commands, a command that does not match a command in the set is flagged as suspicious, and when a command is flagged as suspicious, at least one of an alert, denial of access, limited access, and investigation is performed (see Ramarao, paragraphs 0066, 0056-0057; see also Gruper, column 4, lines 18-30, and column 4, line 65-column 5, line 6).

In reference to Claim 23, the cited art further discloses establishing new categories responsive to observed commands (Ramarao, paragraph 0032, and also Gruper, column 5, lines 32-61) and that the statistical analysis determines whether a predetermined threshold number of new categories has been exceeded and ending the training phase when it is determined that the threshold number has been exceeded (Gruper, column 2, lines 50-63).

In reference to Claim 24, the cited art further discloses ending the training phase responsive to a determination that a predetermined period of time has elapsed (Gruper, column 2, lines 50-63, where the learning mode can have a limited time of operation).

Claims 16, 18, and 19 are directed to software implementations of the methods of Claims 1, 7, and 13, respectively, and are rejected by a similar rationale.

In reference to Claim 21, Applicant admits as prior art the general use of database intrusion detection systems (see page 1, lines 4-17 of the present specification). However, Applicant does not admit the use of real time training of such a database intrusion detection system.

Ramarao discloses a method in which an intrusion detection system has derived a set of acceptable commands (see paragraphs 0056-0057, where there is a list of allowed actions; see also paragraph 0066, where the access control software can be implemented as part of an intrusion detection system) and that during an operation phase, commands that access the database are compared to the set of acceptable commands, and a command that does not match a command in the set is flagged as suspicious (paragraphs 0066, 0056-0057) and that commands in the set of acceptable commands can be stripped of literal field data to produce canonical forms and can be grouped accordingly (paragraph 0032, where parameters can be configured as variable). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the access control portion of the intrusion

detection system (IDS) of Ramarao into the admitted prior art database intrusion detection system, because the application of the general IDS principles disclosed by Ramarao to the admitted prior art database IDS would yield the predictable result of increasing the security of the admitted prior art database IDS by preventing unauthorized actions (see Ramarao, paragraph 0027). However, Ramarao does not explicitly disclose that commands are observed in real time before deriving the set of acceptable commands.

Gruper discloses a method in which a security system includes a learning mode in which commands are observed in order to compile an enforcement file of acceptable actions (column 5, lines 32-61). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the real-time learning mode of Gruper into the admitted prior art database IDS as modified by Ramarao, in order to allow a system to gradually build up knowledge of what actions are and are not to be allowed (see Gruper, column 5, lines 32-47).

11. Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Applicant admitted prior art in view of Ramarao and Gruper as applied to claim 1 above, and further in view of Yaeger, US Patent 5768422.

In reference to Claim 22, the cited art further discloses establishing new categories responsive to observed commands (Ramarao, paragraph 0032, and also Gruper, column 5, lines 32-61) and that any alternative statistical measure may be used for providing limitation to the length of the training mode (Gruper, column 2, lines 59-

62). However, neither Ramarao nor Gruper explicitly discloses using a frequency threshold of establishing categories for the statistical analysis used for ending the training mode. Yaeger discloses a method for training a statistical classifier used for pattern recognition (column 1, lines 7-11, noting that training a security system is a more specific example of pattern recognition; see also column 5, lines 43-45, noting the general applicability to a statistical classifier in any environment) that includes performing a statistical analysis, namely a frequency of learning new patterns (i.e. categories), and ending a training phase of pattern recognition responsive to the statistical analysis (see column 10, line 53-column 12, line 5, where training of a classifier takes place over several phases having lengths that are varied based on the learning rate, which can be variable, see column 8, lines 65-67). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the admitted prior art database as previously modified to incorporate statistical determination of the duration of a training phase, in order to improve the training of the network without a large increase in cost (see Yaeger, column 3, lines 18-22).

12. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Applicant admitted prior art in view of Ramaro, Gruper, and Yaeger.

In reference to Claim 20, Applicant admits as prior art the general use of database intrusion detection systems (see page 1, lines 4-17 of the present

specification). However, Applicant does not admit the use of real time training of such a database intrusion detection system.

Ramarao discloses a software method including a training module in which an intrusion detection system has derived a set of acceptable commands (see paragraphs 0056-0057, where there is a list of allowed actions; see also paragraph 0066, where the access control software can be implemented as part of an intrusion detection system) and groups commands into categories (paragraph 0032, where commands are generalized using variables and grouped accordingly), and a comparison module that compares commands that access the system during an operation phase with commands in the set of acceptable commands (paragraphs 0066, 0056-0057). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the access control portion of the intrusion detection system (IDS) of Ramarao into the admitted prior art database intrusion detection system, because the application of the general IDS principles disclosed by Ramarao to the admitted prior art database IDS would yield the predictable result of increasing the security of the admitted prior art database IDS by preventing unauthorized actions (see Ramarao, paragraph 0027). However, Ramarao does not explicitly disclose that commands are observed in real time before deriving the set of acceptable commands.

Gruper discloses a software method in which a security system includes a training module having a learning mode in which commands are observed in order to compile an enforcement file of acceptable actions and commands are grouped into categories (column 5, lines 32-61, where commands and access rights are grouped into

enforcement files by program), and in which a statistical analysis is performed of the categories and the training phase is ended responsive to that statistical analysis (column 2, lines 50-63, where a time period or number of operations learned is analyzed and used to determine the length of the learning mode). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the real-time learning mode of Gruper into the admitted prior art database IDS as modified by Ramarao, in order to allow a system to gradually build up knowledge of what actions are and are not to be allowed (see Gruper, column 5, lines 32-47). However, although the above prior art discloses that any alternative statistical measure may be used for providing limitation to the length of the training mode (Gruper, column 2, lines 59-62), neither Ramarao or Gruper explicitly discloses using a frequency threshold of establishing categories for the statistical analysis used for ending the training mode.

Yaeger discloses a method for training a statistical classifier used for pattern recognition (column 1, lines 7-11, noting that training a security system is a more specific example of pattern recognition; see also column 5, lines 43-45, noting the general applicability to a statistical classifier in any environment) that includes performing a statistical analysis, namely a frequency of learning new patterns (i.e. categories), and ending a training phase of pattern recognition responsive to the statistical analysis (see column 10, line 53-column 12, line 5, where training of a classifier takes place over several phases having lengths that are varied based on the learning rate, which can be variable, see column 8, lines 65-67). Therefore, it would

have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the admitted prior art database as previously modified to incorporate statistical determination of the duration of a training phase, in order to improve the training of the network without a large increase in cost (see Yaeger, column 3, lines 18-22).

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Grossberg et al, US Patent 5040214, discloses a pattern learning and recognition system that includes a learning phase in which a duration can be varied based on a learning rate.

b. Levy et al, US Patent 7050936, discloses a system in which a learning stage is performed each time a change in a system occurs in order to update a statistical model.

14. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571)272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ZAD/
Examiner, Art Unit 2137

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2137